Appraise of SPIT problem

H. B. Kekre and Sudeep D. Thepade

***Abstract*— Voice over IP (VoIP) technology introduces powerful choices to spammers and telemarketers. Spam over IP Telephony (SPIT) is expected to become a serious problem in the near future. It has the potential to become an even bigger problem than email spam, because the callee will be disturbed by each received SPIT call. For ensuring the success of VoIP it will be crucial to provide effective prevention, particularly in public networks and at gateways between public and enterprise networks. The paper takes quick review across SPIT problem, commercial significance of SPIT to telemarketers, Expectations from SPIT clogging System, Spam scenarios, current solutions**

***Index Terms*—VoIP, Spam, SPIT.**

I. Introduction

Spam is defined as the transmission of bulk unsolicited mails; it is considered to be one of the biggest problems the Internet has ever faced.With the increasing deployment of Internet telephony solutions, often referred to as Voice over IP (VoIP), it is commonly expected that a similar form of spam will affect also this area. This threat is known as SPIT (Spam over Internet Tele phony) and it is defined as the transmission of unsolicited calls over Internet telephony.

Unsolicited bulk calls can take various forms, from telephone polls and sales campaigns, to scams and direct money collection. VoIP technology gives new, advanced tools to telemarketers to increase their productivity: the spectrum ranges from applications for bulk call generation [1] to call centers. With the growth projected and the emergence of inter-domain connectivity, the potential of SPIT to reduce productivity is much higher than email spam, because each SPIT call immediately disturbs the callee by the ringing phone. The damage SPIT can do to voice networks and service varies, from employee distraction and subscriber dissatisfaction, to wasted voicemail space and, in the extreme case, bandwidth [2].

For ensuring the success of VoIP it will be crucial to provide effective prevention, particularly in public networks and at gateways between public and enterprise networks. The transmission of unsolicited calls already exists in the traditional Public Switched Telephone Network (PSTN), where such calls are mostly initiated by telemarketers[5]. However, the high cost of PSTN calls compared to email or VoIP communications limits the attractiveness of this form of advertisement for telemarketers. On the contrary, the costs a spammer would encounter using Internet telephony are substantially lower.

A recent study [1,2] reported that SPIT is roughly three orders of magnitude cheaper to send than traditional PSTN telemarketer calls.

This paper takes an overview of SPIT problem, compares SPIT over PSTN spam, SPIT scenarios and current solution proposals of clogging SPIT.

Dr. H. B. Kekre, Professor, Thadomal Shahani Engineering College, Bandra(w), Mumbai-50, INDIA

Sudeep D. Thepade, , Lecturer, Thadomal Shahani Engineering College, Bandra(w), Mumbai-50, INDIA

hbkekre@yahoo.com, sudeepthepade@gmail.com

II. Comparing Traditional Spam with SPIT

SPIT is a much bigger threat for users than email spam since it will interrupt the users immediately. A SPIT call makes the phone ringing and disturbs the callee. Email spam can be queued in the email program of the receiving user without disturbing the user until he looks at it; even when the mails are checked, the user can process a big number of them in a short amount of time identifying quickly the spam without the need of giving much attention to it. The disturbance in the case of SPIT calls is instead repeated multiple times. Sending SPIT is technically eased by the fact that Internet Telephony protocols and systems have poor identity management (the same technical problem that is present in the mail systems).

An additional problem with SPIT is that most available tech-nologies (coming from email spam prevention) are not useful since:

- the time scale is much different (mails are non-real-time communications while Internet Telephony calls are real-time communications);
- one of the most effective methods (namely content filtering) is not really applicable since the call has to be answered before the content is delivered. Furthermore, automatic methods based on speech recognition are currently too complex and language dependent to be deployed for VoIP calls.

In addition to these simple considerations that give us an overview of the potentiality of the SPIT threat, SPIT will mainly occur in the future because of the reduced costs “SPITters” would encounter in using the Internet Telephony with respect to the PSTN. A simple cost analysis shows how much difference in costs occurs between calls delivered using the PSTN and the public Internet. There are three layers at which we can expect differences in costs between spam over PSTN and over Internet Telephony:

- the costs of the system in terms of software;
- the costs of the system in terms of hardware;
- the costs per spam call;

The costs of the system in terms of software are basically not varying between the two different forms of voice spam (the software could be basically the same, it is just the hardware needed to connect to the network which changes). The costs of the system in terms of hardware are clearly in disfavor of the
PSTN spammer (PSTN cards are much more expensive than network interface cards). As for the costs per spam call, they are in disfavor of the system for sending spam over PSTN because of the higher costs of the PSTN connections; a rough analysis speaks of three order of magnitude lower costs for a SPIT system[2]. Table 1 resumes the costs comparison and clearly shows the costs saving that SPIT systems are offering to possible telemarketers.

Table 1 : Cost Comparisons of PSTN Spam and SPIT [2]

Costs	PSTN Spam	SPIT	Additional Description
Software Cost	A	A	A is depending on the signaling protocol
Hardware Cost	10B-100B	B	B is independent of the signaling protocol
Cost per spam call	About 1000C	C	C is independent of the signaling protocol

III. EXPECTATIONS FROM SPIT PREVENTION SYATEM

The SPIT prevention system has to meet some basic requirements in order to be effective.

- It must minimize the probability of blocking legitimate calls.
- It must maximize the probability of blocking SPIT calls.
- It should minimize the interaction required to the callee to determine whether a call is SPIT.
- It should limit the inconvenience caused to the caller that tries to place a legitimate call.
- It should be general enough to apply to different types of environments (e.g. office, home etc.), different cultures, and languages and so on.

In the literature, several methods have been proposed to prevent SPIT calls; however none of them meets all of these requirements. Besides, most effective methods in preventing SPIT require interaction with the caller and are therefore too intrusive, so that the caller might decide to tear down the call causing the callee to possibly miss important calls. Even worse, other methods require a feedback from the callee. An effective SPIT prevention system must therefore combine the capabilities offered by different component methods, so that the resulting system is able to efficiently block SPIT calls while requiring the least possible interaction with the caller and the callee.

Furthermore, we believe that, being the caller the one that starts the action, he or she is probably more willing to accept a certain level of inconvenience compared to the callee.

IV. SPIT SCENARIOS

The spam detection should be based on three main constituents[3]. First, the observable values of the first Via and Contact headers in the SPIT call set-up requests are valid. Second, spam calls are unidirectional: practically, nobody makes calls towards the spam generator. Third, normally the same conversation party consistently terminates spam calls. This could be the recipient or originator, depending on the scenario:

Scenario A: "Persistent caller". The operator almost never terminates the conversation until the recipient does so. He may be persistent in his offering, or not be allowed to end the conversation first due to a professional code (as in telephone polls). Thus, for this particular caller, statistically call set-up requests go from the originator to recipients, whereas termination requests flow from recipients to this originator.

Scenario B: "Time-conscious caller". The telemarketer tries to cover as many recipients as possible, and hangs up when he figures out that his offer is unlikely to be accepted, which is the most probable case. Therefore, statistically, both call set-up and termination requests go from this source to recipients. Fax broadcasting falls into this category.

Scenario C: "Pre-recorded message". Spam is distributed as a played message. The listener is the one who terminates the call, except in rare cases when he follows the dialing instructions in the message and gets connected to the operator. Statistically, call set-up and termination requests go the same ways as in scenario A.

Scenario D: "Message deposit". The caller can detect a voice mailbox on the recipient side, and then either leave the message or hang up, Wireless Sensor Networks depending on his policy. In either case, both setup and termination requests go from the spammer's side. The events of regular calls and voicemail deposits can be distinguished on the call server, and counted separately. Otherwise, the call termination pattern for scenarios A and C would be corrupted as a result of the mix. Details of SIP signaling for voicemail deposit are described in [20,21,22].

Scenario E: "Call set by third party". A VoIP call between P and Y could be set by X. X could be a spam zombie network element, and P is either telemarketer, or a media server playing a prerecorded message. In SIP, this could be provided either by 3pcc (Third Party Call Control) according to [23].

V. SPECIFIC CHALLENGES AND CURRENT SOLUTION PROPOSALS

There are various difficulties that SPIT detection may face [3,7]. Analyzing data content is impractical, and may also be illegal. The call handling decision must be made in real time, before the actual media session starts, i.e. during the signaling exchange. Since spammers are not interested in service disruption, SPIT is not a Denial of Service (DoS) attack, therefore the techniques used for detection of DoS attacks are hardly applicable: there are no malformed packets, incomplete call set-ups, etc.

For building general SPIT prevention systems with innovative methods, most of the solutions ultimately imply

other providers' capability and, more importantly, intention to have necessary policies and controls in place. Some of the methods does not affect the callee at all and limits the interaction with the caller to an acceptable minimum[2].

Current voice spam solution proposals focus on a few primary approaches: could be given as….

1. **Caller identity accountability** in the access network, and reliable cross-domain authentication [3,7]. This would work if all operators could positively commit to these policies and support the same global standard. Strong authentication is necessary for black/white lists, reputation systems, circles of trust, etc. Rejecting calls from unknown or anonymous sources [19] is part of this approach.
2. **Statistical detection** based on call initiation rates, session duration, and spacing between calls [9,10,11]. Such detection relies on network-specific thresholds, and works for pre - recorded messages only. It also may generate false positive SPIT alarms caused by malicious VoIP signaling floods.
3. **Limited-use addresses**. Users could register disposable IP Telephony URIs (Uniform Resource Identifiers) to use for untrusted initial contacts. As an alias gets compromised by spammers, the owner withdraws it. Extensive user involvement is implied.
4. **Legislative means**. National requirements and registries may not be obeyed by outsourced, off-shore telemarketers. This is especially the case for cheaper, long-distance IP Telephony calls.

VI. REGULATIONS

The present prohibitions for calls include [12,13]: Calls to residences using pre-recorded voice without the prior consent of the called party, except in emergencies; Automatic dialing or pre-recorded messages to any service for which the called party is charged (e.g. cellphones);

- Unsolicited advertisements sent to facsimile machines. It exempts from the restrictions: Callers that have established business relationships with the called party;
- Calls for non-profit purposes (polls, elections, religious talks, fundraising).

Definitions and exceptional cases are still being debated. No specific ruling has been made for IP Telephony as yet[15].

VII. CONCLUSION

It is clear from existing data networks that spam is a massive industry, based on a combination of commercial and malicious intent. There is every indication that the same intent, efforts and technology will be expanded to become a clear threat to IP-based communications services. The particular problem of SPIT will emerge on a large scale as VoIP technologies become extensively adopted with inter-domain connectivity. The solution proposals available today are either incomplete, or essentially rely on the ubiquitous adoption of common controls and standards. As IP PBXs, Gateways, Softswitches, and other components are integrating additional security functionality, protection from voice spam will make them a market differentiator. Carriers and products providing voice network interconnection will be expected to offer a solution.

VIII. REFERENCES

[1]. J. Rosenberg et al., "The Session Initiation Protocol (SIP) and Spam," draftietf-sipping-spam-01.txt, July 2005.
[2]. Juergen QUITTEK, Saverio NICCOLINI, Sandra TARTARELLI, Roman SCHLEGEL, "Prevention of Spam over IP Telephony (SPIT)", NEC Technical journal, Vol.1 No.2, 2006, pp. 114-119
[3]. Srinivas Mantha Fiete, S. Vathsal Fiete , "IP TELEPHONY NETWORKS – BLOCKING SPAM", Proc. of the International Conference on Network Security 2007 (ICONS 2007), Tamil Nadu, India, 29-31 January 2007.
[4]. MarTel International, Inc., PreEmptive Dialer.
[5]. Privacy Rights Clearinghouse, "Prerecorded Telemarketing Calls to Those with an Existing Business Relationship (EBR): Comments to the Federal Trade Commission,", January 2005.
[6]. [3] K. Srivastava and H. Schulzrinne, "Preventing Spam for SIP-based Instant Messages and Sessions," Columbia University Technical Report CUCS-042-04, October 2004.
[7]. J. Rosenberg, C. Jennings and J. Peterson, "The Session Initiation Protocol (SIP) and Spam," IETF draft, July 2005.
[8]. R. Sparks, "The Session Initiation Protocol (SIP) Refer Method," IETF RFC 3515
[9]. D. Shin and C. Shim, "VoIP Spam Control with Gray Leveling", 2nd Workshop on Securing Voice over IP, June 2005.
[10]. Borderware Technologies Inc., SIPassure(tm) SIP Firewall.
[11]. Eyeball Networks Inc., Anti-SPIT(tm) Server.
[12]. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227.
[13]. Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014 (2003)
[14]. www.fcc.gov/cgb/policy/telemarketing.html
[15]. http://ndncregistry.gov.in/ndncregistry/index.jsp
[16]. The Federal Trade Commission, the National Do Not Call Registry.
[17]. Directive on Privacy and Electronic Communications 2002/58/EC of the European Parliament and of the Council of 12 July 2002.
[18]. Statutory Instrument 2003 No. 2426, UK Office of Public Sector Information.
[19]. BellSouth Corp., Privacy Director(r) Service
[20]. J. Rosenberg et al., "SIP: Session Initiation Protocol," IETF RFC 3261.
[21]. [16] J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)," IETF RFC 3323.
[22]. B. Campbell and R. Sparks, "Control of Service Context using SIP Request-URI," IETF RFC 3087.
[23]. J. Rosenberg et al., "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)," IETF RFC 3725.

IX. BIOGRAPHIES

Dr. H. B. Kekre has received B.E. (Hons.) in Telecomm. Engg. from Jabalpur University in 1958, M.Tech (Industrial Electronics) from IIT Bombay in 1960, M.S.Engg. (Electrical Engg.) from University of Ottawa in 1965 and Ph.D.(System Identification) from IIT Bombay in 1970. He has worked Over 35 years as Faculty in Electrical Engg.and HOD Computer science and Engg. at IIT Bombay. From last 11 years working as a professor in Dept. of Computer Engg. at Thadomal Shahani Engg. College, Mumbai. His areas of interest are Digital Signal processing and Image Processing. He has more than 150 papers in National/International Conferences/Journals on his credit

Sudeep D. Thepade has Received B.E.(Computer) degree from North Maharashtra University with Distinction in 2003, currently has submitted the project work for M.E. in Computer Engineering, University of Mumbai. He has more than 4 years of experience in teaching. Currently is working as a lecturer in Dept. of Information Technology at Thadomal Shahani Engg. College, Mumbai. His areas of interest are Image Processing and Computer Networks. He has 13 papers in National/International Conferences on his credit